

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-269022

(43)Date of publication of application : 25.09.2003

(51)Int.Cl.

E05B 49/00
B60R 25/00

(21)Application number : 2002-073376

(71)Applicant : ADVANCE DESIGN CORP

(22)Date of filing : 15.03.2002

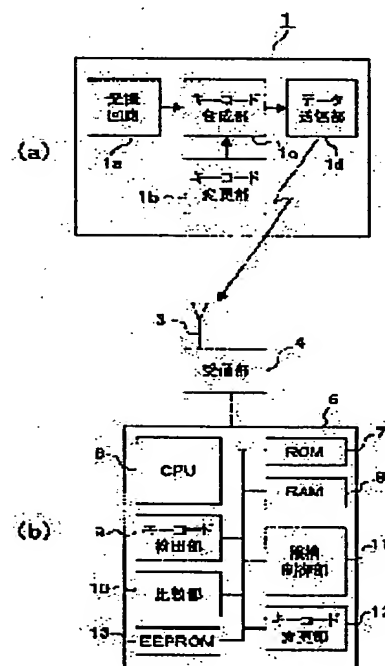
(72)Inventor : HONDA TADASHI

(54) BURGLARPROOF SYSTEM FOR VEHICLE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a burglarproof system for vehicles making it difficult to decode a key code and efficiently preventing burglaries of vehicles (cars) even when infrared rays or radio waves are received by a third person when a door is locked or unlocked.

SOLUTION: A transmitting unit (remote controller) outputs information including key codes to a vehicle (car) and in the vehicle (car), coincidence of the key codes is judged to release the door lock. In this case, the key code is changed by operating a starter key of an engine and the key code is changed in compliance with the above in the transmitting unit (remote controller) side. Accordingly, the key code does not coincide with another one even if the third person gets the key code and transmits information including the key code to the vehicle (car), key codes do not coincide and hence, the door lock can not be released.



LEGAL STATUS

[Date of request for examination]

14.03.2005

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-269022

(P2003-269022A)

(43) 公開日 平成15年9月25日 (2003.9.25)

(51) Int.Cl. ⁷	識別記号	F I	データベース(参考)
E 0 5 B 49/00		E 0 5 B 49/00	K 2 E 2 5 0
			M
B 6 0 R 25/00	6 0 6	B 6 0 R 25/00	6 0 6

審査請求 未請求 請求項の数 8 OL (全 7 頁)

(21) 出願番号 特願2002-73376(P2002-73376)

(22) 出願日 平成14年3月15日 (2002.3.15)

(71) 出願人 500340990

アドバンス・デザイン株式会社

神奈川県川崎市川崎区浅野町4丁目13番地

(72) 発明者 本田 正

神奈川県川崎市川崎区浅野町4丁目13番地

アドバンス・デザイン株式会社内

(74) 代理人 100103148

弁理士 山本 輝美

Fターム(参考) 2E250 AA21 B808 B865 D006 EE08

EE09 EE10 FF25 FF36 FF38

GG06 GG14 HH02 JJ03 KK03

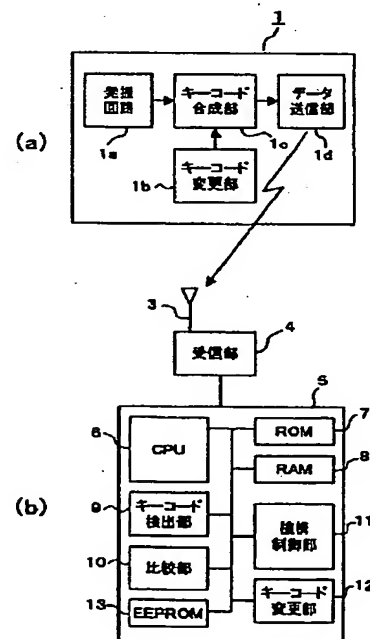
LL01

(54) 【発明の名称】 車両盗難防止システム

(57) 【要約】

【課題】 本発明は車両盗難防止装置に関し、特にドアの施錠又は開錠の際に、赤外線や電波が第三者に受信された場合でも、キーコードの解読を困難とし、車両（自動車）の盗難を有効に防止する車両盗難防止システムを提供するものである。

【解決手段】 送信ユニット（リモコン）はキーコードを含む情報を車両（自動車）に送信し、車両（自動車）ではキーコードの一致を判断してドアロックを解除する。この場合、キーコードはエンジンのスタータキーを操作することによって変更され、送信ユニット（リモコン）側でも対応してキーコードが変更される。したがって、第三者が例えばキーコードを知って車両（自動車）に当該キーコードを含む情報を送信してもキーコードが一致せずドアロックを解除することができない。



【特許請求の範囲】

【請求項1】 キーコードを含む情報を送信する送信ユニットと、
該送信ユニットから送信される情報を受信する受信ユニットと、
該情報から前記キーコードの解析を行う解析部と、
該解析部の解析の結果得られるキーコードと、車両側で保持するキーコードとの一致を判断する判別手段と、
該判別手段の判別結果が一致する時、ドアロックを解除する解除手段と、
該ドアロックの解除後、キーコードの変更処理を行う変更手段と、
を有することを特徴とする車両盗難防止装置。

【請求項2】 前記キーコードの変更処理は、前記送信ユニット側でも同じ変更処理を行うことを特徴とする請求項1記載の車両盗難防止装置。

【請求項3】 前記キーコードの変更処理は、所定時間の経過に基づいて実行されることを特徴とする請求項2記載の車両盗難防止装置。

【請求項4】 前記キーコードの変更処理は、リングカウンタを使用して行うことを特徴とする請求項1、2、又は3記載の車両盗難防止装置。

【請求項5】 キーコードを使用して署名処理を行い、該署名結果を送信する送信ユニットと、
該送信ユニットからの送信を受信する受信ユニットと、
前記署名情報の検証を行い、得られる結果が一致する時、ドアロックを解除する解除手段と、
該ドアロックの解除後、キーコードの変更処理を行う変更手段と、
を有することを特徴とする車両盗難防止装置。

【請求項6】 前記送信ユニットは受信手段も備え、前記変更されたキーコードを受信し、次の署名処理に使用することを特徴とする請求項5記載の車両盗難防止装置。

【請求項7】 前記送信ユニットは受信手段も備え、前記変更されたキーコードをネットワークを介して受信し、次の署名処理に使用することを特徴とする請求項6記載の車両盗難防止装置。

【請求項8】 前記署名処理にはDESの暗号化アルゴリズムが使用されることを特徴とする請求項5、6、及び7記載の車両盗難防止装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は車両盗難防止装置に関する。

【0002】

【従来の技術】 今日、利便性の面から自動車のドアをキーを使用せずに施錠、開錠するキーレスエントリーシステムが開発されている。現在このシステムは、高級車から軽乗用車まで広く使用され、特に赤外線を使用したシ

ステム、又は電波（電磁波）を使用したシステムが主流である。

【0003】 例えば、赤外線を使用する場合、ガリウムや砒素等の材料で形成された発光素子を有する送信ユニット（リモコン）から車両（自動車）の受光部に情報（キーコード）を送り、情報（キーコード）の一致を判断してドアの開錠を行う。また、電波を使用する場合、送信ユニット（リモコン）から車両（自動車）に取り付けられるアンテナに情報（キーコード）を送り、受信ユニットでキーコードの解析を行い、一致を判断してドアの開錠を行う。尚、上記電波による場合には、RF電磁波が使用される。

【0004】 従って、上記何れのキーレスエントリーシステムにおいても、利用者は車両（自動車）に近づき、送信ユニット（リモコン）を操作し、キーコードを含む情報を車両（自動車）に送信し、車両（自動車）のドアロックを解除する。

【0005】

【発明が課題するための課題】 上記従来のシステムにおいて使用される赤外線、又は電波は微弱であり、許されている送信出力には限りがある。しかし、車両の周囲のどの方向から操作されても、1m以上の距離で作動しなければならない。また、実力として、3m以上離れた距離でも作動することが要求される。この為、施錠又は開錠の際に、赤外線や電波が第三者に受信される場合もある。

【0006】 特に、車両（自動車）の窃盗目的で受信が不法に行われ、キーコードの解読が行われると、車両（自動車）の窃盗行為が容易に可能になる。そこで、本発明は上記従来の実情に鑑み、ドアの施錠又は開錠の際、赤外線や電波が第三者に受信された場合でも、キーコードの解読を困難とし、車両（自動車）の盗難を有効に防止する車両盗難防止システムを提供するものである。

【0007】

【課題を解決するための手段】 上記課題は、請求項1記載の発明によれば、キーコードを含む情報を送信する送信ユニットと、該送信ユニットからの送信を受信する受信ユニットと、前記キーコードの解析を行う解析部と、該解析部の解析結果得られるキーコードと車両側で保持するキーコードとの一致を判断する判別手段と、該判別手段の判別結果が一致する時、ドアロックを解除する解除手段と、該ドアロックの解除後、スターターキーの操作に従ってキーコードの変更処理を行う変更手段とを有する車両盗難防止装置を提供することによって達成できる。

【0008】 ここで、上記送信ユニットは所謂リモコンであり、キーコードを含む情報を赤外線、又は電波にのせて車両（自動車）の受信ユニットに送る。したがって、受信ユニットは赤外線によってキーコードが送られ

た場合、フォットトランジスタ等の受光素子によって情報を受信し、電磁波によって送信された場合にはアンテナによって情報を受信する。

【0009】解析部は情報の解析を行い、キーコードを抽出し、予め車両（自動車）側の例えばコンピュータが保持するキーコードとの一致を判断し、一致している場合ドアロックを解除する。そして、その後行うスターキーの操作に基づいてキーコードの変更処理を行う。

【0010】このように構成することにより、本例のシステムで使用するキーコードは順次変更され、次のキーレスエントリーにおいて同じキーコードが使用されることがなく、例えばキーコードが解読され、ドアロックの解除に使用されてもキーコードが不一致となり車両の盗難を防止できる。

【0011】また、車両（自動車）の所有者は次にドアロックの解除の際、キーコードが一致せず、解除できない場合不正なアクセスが行われたことを知る。請求項2の記載は、上記請求項1記載の発明において、前記キーコードの更新処理は、前記送信ユニット側でも同じアルゴリズムによって行われる。

【0012】このように構成することにより、車両（自動車）の所有者は、例えばキーコードが車両（自動車）側で変更されたとしても問題なくドアロックの解除を行うことができる。

【0013】請求項3の記載は、上記請求項2の記載において、前記キーコードの更新処理は、所定時間の経過に基づいて実行される。このように構成することにより、ドアロックを開錠した後、エンジンを始動しない場合でも、所定周期でキーコードが更新される。したがって、例えば車両（自動車）に荷物を取りに行く為ドアロックを解除する行為のみを行うような場合でも、自動的にキーコードは時間の経過と共に変更されており、車両の盗難を有効に防止できる。

【0014】請求項4の記載は、上記請求項1、2、又は3の記載において、前記キーコードの更新は、リングカウンタを使用して行う構成である。この場合、車両（自動車）側と送信ユニット（リモコン）側で同じリングカウンタを使用する。

【0015】上記課題は、請求項5記載の発明によれば、キーコードを使用して署名処理を行い、該署名結果を送信する送信ユニットと、該送信ユニットからの送信を受信する受信部と、前記署名情報の検証を行い、得られる結果が一致する時、ドアロックを解除する解除手段と、該ドアロックの解除後、キーコードの更新処理を行う更新処理手段とを有する車両盗難防止装置を提供することによって達成できる。

【0016】ここで、署名処理には上記キーコードを含む情報によって暗号化を行い、途中で第三者の介入を排除する。例えば、信号を解読してキーコードを得たとしても、署名のアルゴリズムを知らなければ暗号化してキ

ーコードを車両（自動車）に送信することができない。このように構成することによっても、有効に車両盗難を防止できる。

【0017】請求項6の記載は、上記請求項5の記載の発明において、前記送信ユニットは受信手段も備え、前記更新されたキーコードを受信し、次の署名処理に使用する構成である。

【0018】このように構成することにより、次の署名処理の際には更新されたキーコードが使用され、例えば第三者が前に送信された情報をそのまま車両（自動車）に送信しても検証結果が一致せず、更に有効に車両の盗難防止が可能となる。

【0019】請求項7の記載は、上記請求項5の記載の発明において、前記送信ユニットは受信手段も備え、前記更新されたキーコードをネットワークを介して受信し、次の署名処理に使用する構成である。

【0020】ここで、ネットワークはインターネット等のネットワーク網であり、このように構成することによっても、車両の盗難を防止できる。請求項8の記載は、上記請求項5、6、及び7の記載において、前記署名処理にはDESの暗号化アルゴリズムを使用する構成である。

【0021】

【発明の実施の形態】以下、本発明の実施の形態を図面を参照しながら説明する。

<第1の実施形態>図1は、本実施形態のシステム構成を説明する図である。同図において、1は送信ユニット（リモコン）であり、RF電波を車両（自動車）2に出力する。車両（自動車）2には、アンテナ3、受信ユニット4、制御部5が設けられ、RF電波はアンテナ3によって受信され、受信ユニット4によって制御部5に送られる。

【0022】図2（a）は上記送信ユニット（リモコン）1の内部構成を説明する図であり、発振回路1a、キーコード変更部1b、キーコード合成部1c、データ送信部1dで構成されている。キーコード合成部1cは、キーコード変更部1bから供給されるキーコードを発振回路1aの発振信号を使用して変調し、例えばシステムコード、及びキーコードデータを作成してデータ送信部1dに出力する。データ送信部1dは作成された上記システムコード及びキーコードデータを車両（自動車）2のアンテナ3に送信する。

【0023】一方、図2（b）は車両（自動車）2側の構成であり、アンテナ3、受信ユニット4を含む制御部5の構成を説明する図である。同図において、制御部5はCPU6、ROM7、RAM8、キーコード検出部9、比較部10、機構制御部11、キーコード変更部12、及びEEPROM13で構成され、CPU6はROM7のプログラムによって制御を行い、このROM7にはキーレスエントリーの制御プログラムも記憶されてい

る。また、RAM8はCPU6のワークエリアであり、本例の制御において発生するデータを記憶する。

【0024】キーコード検出部9は受信ユニット4から供給されるデータからキーコードを検出する。また、比較部10はキーコード検出部9が検出したキーコードと正規のキーコードの比較を行い、一致又は不一致の判断を行う。

【0025】キーコード変更部12はキーコードの更新処理を行う機能を有し、変更後のキーコードはEEPROM13に記憶される。一方、機構制御部11は車両（自動車）の各部に接続され、制御信号を送信すると共に、センサから信号を受信する。例えば、図3に示すように、機構制御部11は各種ランプ18、ドアロック部19、ヒータ14、方向指示器15等に接続され、ドライバの方向指示を検出するセンサ16やドライバのブレーキ操作を検出するブレーキセンサ等の各種センサにも接続されている。

【0026】そして、機構制御部11は、例えば前照灯やテールランプ等のランプ18に点灯信号を送り、ドアロック部19に施錠又は開錠指示信号を出力する。また、ヒータ14に対して加熱信号を送信し、方向指示器に指示信号を送信する。また、ドライバーの操作信号を受信し、対応する制御を行う。例えば、ドライバーのブレーキ操作に従って、当該操作をセンサで検出し、機構制御部11に供給する。

【0027】以上の構成において、以下に本例の処理動作を説明する。図4は本例の処理を説明するフローチャートである。同図において、先ず車両（自動車）2を運転する為、ドライバーは車両（自動車）に近づき送信ユニット（リモコン）1の所定キーを押す（ステップ（以下、Sで示す）1）、送信ユニット（リモコン）1からRF電波をアンテナ2に送る（S2）。

【0028】一方、車両（自動車）に設置された受信ユニット4はRF電波の受信を判断し（S3）、RF電波が供給されるとキーコードを抽出する（S4）。そして、抽出したキーコードと車両（自動車）側で記憶するキーコードを比較する（S5）。尚、車両（自動車）側のキーコードは前述のEEPROM13に記憶され、後述するキーコード変更部12によって順次変更されたキーコードである。

【0029】ここで、両コードが一致していると判断すると、CPU6は機構制御部11に制御信号を出力し（S6）、機構制御部11からドアロック部13にロック解除信号を出力し、ドアロックの解除が行われる（S7）。

【0030】次に、ドライバはドアを開け運転席に座り、スタートキーを回してエンジンを始動する。図5は以後の処理を説明するフローチャートである。先ず、ドライバがキーシリンダにキーを差し込みスタートキーを回すと、エンジンが始動し、同時にキー操作信号が機構

制御部11を介してCPU6に送られる（S8、S9）。CPU6は上記キー操作信号が供給されると、キーコード変更要求をキーコード変更部12に送り、キーコードの変更要求を行う（S10）。

【0031】ここで、キーコード変更部12は、例えばリングカウンタで構成され、1→2→3・・・→9→0→1・・・とカウンタを順次循環出力する構成である。したがって、例えば前のキーコードが***1であった場合、リングカウンタは次に***2を出力する。したがって、この場合キーコード変更部12の出力は***2のキーコードとなる。また、前のキーコードが***7であった場合、リングカウンタは次に***8を出力し、キーコード変更部12の出力は***8となる。

【0032】このようにして出力された変更後の新たなキーコードはEEPROM13に記憶され、次のキーコードの比較に備える。すなわち、前のドアロックの解除の際、例えば第三者が電波を傍受し、キーコードを解読した場合、不法に当該キーコードを使用して車両（自動車）のドアロックを解除しようとする。しかし、比較部10がキーコードの比較を行う際、一方は更新前のキーコードであり、他方は更新後のキーコードであり、不一致となる。したがって、ドアロックは解除されず、車両の盗難を未然に防ぐことができる。

【0033】尚、車両（自動車）の所有者がドアロックを解除する場合には、正規の送信ユニット（リモコン）を使用するので、キーコードの更新処理が行われ、キーコードが一致するのでドアロックの解除することができる。

【0034】また、第三者による不法なアクセスがあった場合、キーコードが一致せずドアロックの解除を行うことはできないが、キーコードの更新処理のみを実行する構成とする。すなわち、図7に示すようにキーコードが不一致の場合、キーコードの変更要求を行い（ステップ（以下、Wで示す）1）、キーコードを更新し（W2）、EEPROM13に記憶する（W3）。

【0035】このように構成することにより、不法アクセスがあった場合、正規の車両（自動車）の所有者がドアロックを解除しようとする場合でも、ドアの解除を行うことができず、ドアロック解除の不法アクセスがあったことが判明する。

【0036】尚、上記実施形態に説明においても、電波を使用した例について説明したが、赤外線を利用するシステムにおいても同様に適用できる。また、キーコード変更部12はリングカウンタを使用する場合だけではなく、他の構成であってもよい。例えば、予め送信ユニット（リモコン）1側との間で取り決めたアルゴリズムに従ってキーコードを生成し、利用する構成としてもよい。

【0037】＜第2の実施形態＞次に、本発明の第2の実施形態について説明する。本例は、キーコードを使用

して署名処理を行い、この情報を車両（自動車）側に送信する構成である。本例においても、図1に示すように送信ユニット（リモコン）1、アンテナ3、受信ユニット4、制御部5の構成は同様である。但し、送信ユニット（リモコン）1の内部構成、及び制御部5の内部構成が異なる。以下、具体的に説明する。

【0038】図8は本例で使用する送信ユニット（リモコン）1'の内部構成であり、発振回路1a、キーコード変更部1b、キーコード合成部1c、データ送信部1d、更に署名処理部1fで構成されている。本例においては、署名処理部1fが追加されている。この署名処理部1fは前述のキーコード変更部1bから出力されるキーコードを基に署名処理するものであり、図9に構成を示す。

【0039】すなわち、DES（data encryption standard）のアルゴリズムを使用し、上記キーコード（DATA）を特定のキーを使用して暗号化し、前述のキーコード合成部1cに送る。ここで、上記特定のキー（DATA）は車両（自動車）側で検証の際使用するキーと同じである。

【0040】キーコード合成部1cは署名処理部1fで暗号化したデータを発振回路1aからの発振信号によって変調し、データ送信部1dを介してアンテナ3に送信する。

【0041】車両（自動車）2の制御部5は、アンテナ3、受信ユニット4を介して供給される情報の検証処理を行い、同じDESのアルゴリズムを使用してキーコードを抽出する。

【0042】このようにして抽出されたキーコードは前述と同様、正規のキーコードと比較され、両コードが一致していれば機構制御部11に制御信号を出力し、ドアロック部13にロック解除信号が出力し、ドアの施錠を解除する。一方、両コードが不一致であれば、ドアの施錠が解除されず、車両の盗難を防止できる。

【0043】尚、本例においても、スタートキーを回しエンジンが始動すると、前述の図5に示すように、キーコードの変更処理が行われる。この変更処理は、送信ユニット（リモコン）1のキーコード変更部1bにおいても同じ処理が行われ、次にキーレスエントリーを行う際、新たなキーコードによって署名処理が行われ、ドアロックを解除することができる。

【0044】以上のように処理することによって、例えば第三者が電波を傍受し、キーコードを解読した場合でも、盗聴者は特定キーが分からず車両（自動車）2に対して署名データを送信することができない。

【0045】また、DESの暗号化手法にも各種方法が存在し、完全に一致したアルゴリズムを使用して署名データを作成することは困難であり、車両の盗難を有効に防止することができる。

【0046】尚、署名データを完全にコピーして使用す

る場合でも、本例の場合キーコードが毎回変更されており、全く同じ署名データを車両（自動車）2に送信することは不可能である。したがって、より確実に車両の盗難防止を図ることができる。

【0047】尚、上記実施形態に説明においても、電波に限らず赤外線を使用する場合でも適用できる。

【0048】

【発明の効果】以上詳細に説明したように、本発明によれば、例えばキーコードが解読され、ドアロックの解除に使用されてもキーコードが不一致となり車両盗難を防止できる。

【0049】また、署名処理を使用することによってキーコードの解読を困難とし、有効に車両盗難を防止できる。

【図面の簡単な説明】

【図1】本実施形態のシステム構成を説明する図である。

【図2】（a）は送信ユニット（リモコン）の構成を説明する図であり、（b）は車両（自動車）側の構成であり、アンテナ、受信ユニットを含む制御部の構成を説明する図である。

【図3】機構制御部の構成を説明する図である。

【図4】第1の実施形態の処理を説明するフローチャートである。

【図5】第1の実施形態の処理を説明するフローチャートである。

【図6】リングカウンタの構成を説明する図である。

【図7】第1の実施形態の変形例の処理を説明するフローチャートである。

【図8】第2の実施形態で使用する送信ユニット（リモコン）の構成を説明する図である。

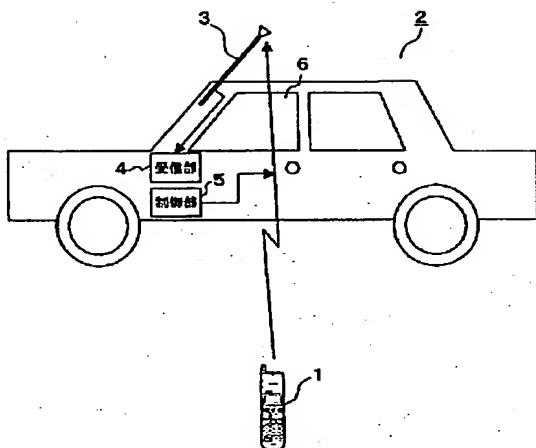
【図9】署名処理を説明する図である。

【符号の説明】

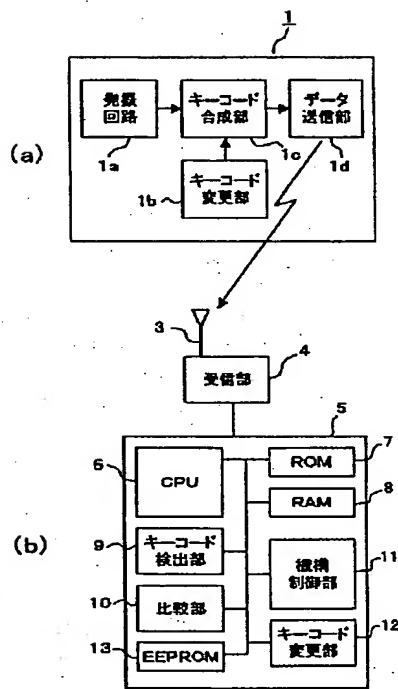
- 1 送信ユニット（リモコン）
- 1a 発振回路
- 1b キーコード変更部
- 1c キーコード合成部
- 1d データ送信部
- 1f 署名処理部
- 2 車両（自動車）
- 3 アンテナ
- 4 受信ユニット
- 5 制御部
- 6 CPU
- 7 ROM
- 8 RAM
- 9 キーコード検出部
- 10 比較部
- 11 機構制御部
- 12 キーコード変更部

13 EEPROM

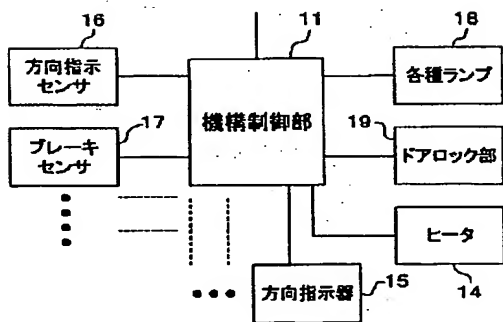
【図1】



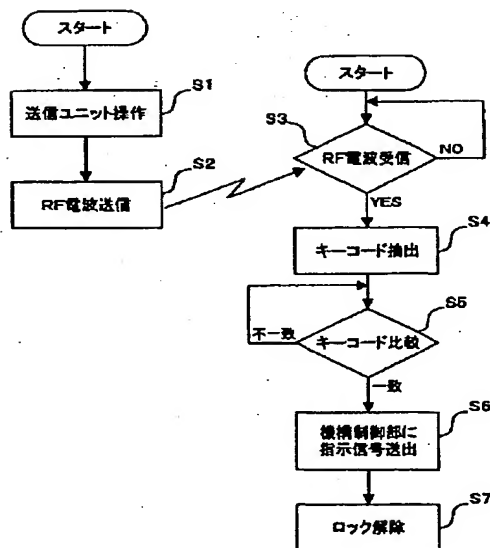
【図2】



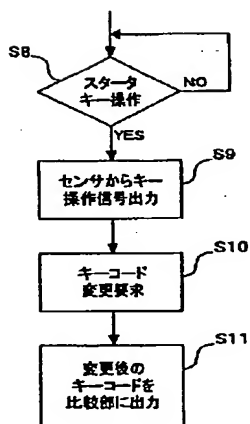
【図3】



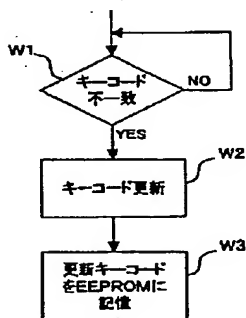
【図4】



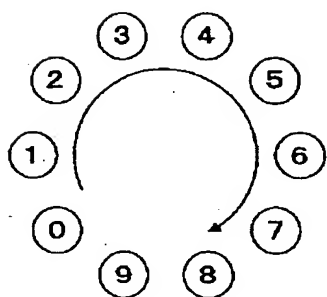
【図5】



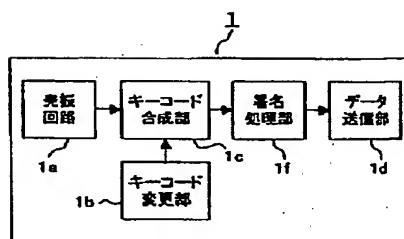
【図7】



【図6】



【図8】



【図9】

